



We live in a networked world, and a networked Navy-Marine Corps team has become a reality. Information sharing with collaboration across command elements and national boundaries, coupled with increasing speed, accuracy and efficiency, characterize this 21st century network-centric environment.

Network-centric warfare creates a decisive warfighting advantage to sustain our continued maritime dominance. However, network-centric warfare also has the potential to expose vulnerabilities. Compromised identity of personnel, systems and services could be catastrophic in both strategic and tactical warfighting operations. Furthermore, the global war on terrorism is redefining network and data sharing boundaries. With the likely potential for those boundaries to continue expanding, Identity Protection and Management (IPM) becomes more critical as a means to support information sharing with authenticity and non-repudiation.

Identity protection, or safeguarding of identities, and the sensitive information that characterize people, systems and services, is a crucial capability in a network-centric warfighting environment. IPM enables the Department of Defense (DoD) to realize joint information superiority, both on and off the battlefield, and it will enable secure, integrated, interoperable and scalable information sharing solutions for people, systems and services in a network-centric warfare environment. Sound IPM must leverage the evolution and convergence of robust capabilities associated with biometrics, smart card, Public Key Infrastructure (PKI), Radio Frequency Identification (RFID) and other technologies, to positively assert and strongly protect trusted identities, processes and assets with integrity.

Our Department of Defense joint warfighting team has already made great progress on this front. Accomplishments thus far include:

- Issuance of over 4.5 million Common Access Cards (CACs) and over 14.5 million DoD PKI certificates
- Enablement of DoD Web sites to use Secure Socket Layer protocol for non-public communications
- Adoption of the FBI's Integrated Automated Fingerprint Identification System standard as the DoD method for collecting, exchanging and validating fingerprint biometrics data of detainees, enemy combatants, and persons of interest

The DON is expanding IPM initiatives to include enabling unclassified networks to support cryptographic logon from DoD PKI credentials stored on CACs, and requiring PKI credentials rather than passwords for Web site access. We are rapidly approaching a future where the information sharing that enables maritime dominance is secure and trusted.

Our commitment to a robust identity management solution across the Department of Defense will serve as the crucial foundation to achieve our vision of network-centric operations and knowledge dominance.

Dave Wennergren



DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER
W W W . D O N C I O . N A V Y . M I L